CLAIMS

1. A system for detecting fraudulent transactions, comprising:

an interface for inputting transaction data and outputting analysis results; and

a secure data processing unit (SDPU) that provides a secret and tamper-proof computing environment, wherein the SDPU includes:

a security system that can restrict access to data and program execution;

an analysis system for analyzing inputted transactions;

a plurality of surveillance algorithms stored in an encrypted database; and

a selection program for selecting at each of a sequence of random times a different surveillance algorithm to be used by the analysis system.

2. The system of claim 1, wherein the SDPU further includes an algorithm performance system that assists the selection program in selecting surveillance algorithms.

3. The system of claim 1, wherein the selection program utilizes a random selection process for selecting surveillance algorithms.

4. The system of claim 1, wherein the security system prevents observation of the operational behavior of the SDPU.

5. The system of claim 1, wherein the security system includes an encryption system for encrypting and decrypting data.

6. A method for detecting fraudulent transactions, comprising:

providing an interface for inputting transaction data and receiving analysis results;

providing a secure data processing unit (SDPU) that provides a secret and tamper-proof computing environment, wherein the SDPU can restrict access to data and program execution;

providing a plurality of surveillance algorithms stored in an encrypted database;

analyzing inputted transactions for fraud with a surveillance algorithm within the SDPU; and

selecting a different surveillance algorithm from the plurality of surveillance algorithms to be analyze future inputted transactions.

7. The method of claim 6, wherein the step of selecting a different surveillance algorithm utilizes a random selection process.

8. The method of claim 7, comprising the further steps of:

measuring algorithm performance; and

using the measured performance in selecting surveillance algorithms.

9. The method of claim 8, comprising the further steps of:

measuring a randomness of the algorithm selection process using a technique selected from the group consisting of correlation and entropy measures; and

issuing an alert is the randomness goes under a predetermined threshold.

10. The method of claim 6, wherein the SDPU prevents observation of which surveillance algorithm is selected.

11. The method of claim 6, including the further step of decrypting the selected surveillance algorithm.

12. A confederated fraud detection system, comprising:

an interface for inputting transaction data; and

a secure data processing unit (SDPU) that provides a secret and tamper-proof computing environment, wherein the SDPU includes:

a security system that can restrict access to data and program execution;

a consolidated database for storing encrypted data from a plurality of members;

a consolidation system for securely importing encrypted data from each of the plurality of members; and

at least one data analysis tool for analyzing the consolidated database.

13. The confederated fraud detection system of claim 12, further comprising a set of data access rules that determines access criteria to data stored in the consolidated database.

14. The confederated fraud detection system of claim 12, further comprising a secure data communication channel through which data traffic can remain secret.

15. The confederated fraud detection system of claim 12, further comprising an encryption system for decrypting imported data, wherein the encryption system includes a system for protecting encryption keys.

16. The confederated fraud detection system of claim 12, further comprising an analysis system for analyzing inputted transactions, wherein the interface allows for securely inputting transaction data to be analyzed and for securely outputting analysis results.

17. The confederated fraud detection system of claim 16, wherein the analysis system utilizes a probabilistic sampling method wherein an acceptance probability is proportional to a measure of fraud cost of the analyzed transaction.

18. The confederated fraud detection system of claim 17, wherein the data set needed to implement the probabilistic sampling method is small enough to fit in a memory space of a secure processor.

19. The confederated fraud detection system of claim 12, wherein the at least one data analysis tool includes a system for building models.

20. The confederated fraud detection system of claim 12, further comprising a battery of secure processors capable of providing a set of functions that are deemed to require high security, high confidentiality, or high privacy.

21. A method for implementing a fraud detection service, comprising:

providing a member based fraud detection service;

securely transferring data to a confederated fraud detection system from a member such that the data is maintained as confidential;

storing the data in an encrypted form in a consolidated database along with data from other members;

using the data in the consolidated database to facilitate fraud detection; and

performing fraud detection on at least one transaction in a secure manner that is confidential with regard to the other members.

22. The method of claim 21, wherein the data is transferred to the fraud detection service in an encrypted form.

23. The method of claim 22, wherein the data transferred to the fraud detection service is decrypted by the fraud detection service, verified for accuracy, and approved for storage.

24. The method of claim 21, wherein each member has the option of allowing their data to be used in conjunction with data from other members for a purpose selected from the group consisting of: constructing a model and performing fraud detection.

25. The method of claim 21, further comprising providing a secret surveillance service to the members, wherein the service includes:

providing a model comprising a library of surveillance programs; and

running different surveillance programs at different times so that an outside party cannot detect which surveillance program is running.

26. The method of claim 21, further comprising providing a data processing service to the members, wherein the service includes:

providing data consolidation services;

providing model construction services; and

providing transaction analysis services.

27. The method of claim 21, wherein the confederated fraud detection system comprises a data management system that is programmable, tamper resistant, tamper sensitive, tamper reactive and tamper evident.

28. The method of claim 21, comprising the further step of causing random data to be received by the fraud detection service in order to ensure that secrecy is not lost to a third party observing traffic to the fraud detection service.

29. The method of claim 21, wherein an iterative selective sampling method for selecting subsets of analysis data is employed by the fraud detection service in performing fraud detection so that the analysis data used in each iteration of fraud detection is small enough to be stored in the memory of a secure processor.

30. The method of claim 29, wherein the iterative selective sampling method includes a probabilistic sampling method with acceptance probability proportionate to a measure of fraud cost of each transaction record.

31. The method of claim 21, wherein the fraud detection service includes a system for reconstructing activity networks among participating members to identify suspicious patterns.

32. The method of claim 21, wherein confidentiality of the data is controlled by rules established within a rules engine.

33. The method of claim 21, wherein the fraud detection service includes audit capabilities for replicating analysis activities performed by the fraud detection service.

34. The method of claim 33, wherein the audit capabilities include a system for maintaining secrecy of which algorithms were used during the analysis activities.

35. A distributed fraud detection system, comprising:

a plurality of secure data processing unit (SDPU) distributed among a set of members, wherein each SDPU provides a secret and tamper-proof computing environment for the member, and wherein the SDPU includes:

a secure database for storing member data;

a security system that can restrict access to member data; and

a secure communication system for securely transferring member data to and from each of the plurality of members in a secure and confidential manner.

36. The distributed fraud detection system of claim 35, wherein at least one of the SDPUs includes a data analysis tool for analyzing data distributed among the members in order to build a model for detecting fraud.

37. The distributed fraud detection system of claim 35, wherein at least one of the SDPUs includes a transaction analysis tool for analyzing an inputted transaction for fraud by collecting data distributed among the members.